Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A tangible machine readable medium, comprising:

a writeable area of the medium;

a read only area of the medium;

a content stored on the writeable area of the medium;

a first media validation data containing an encrypted preselected value and being stored on the writeable area; and,

a second media validation data equal to the first media validation data and being stored on the read only area.

2. (currently amended) The ~~medium of claim 1~~ device of claim 4, further comprising:

a circuit to calculate a message authentication code over the first media validation data using a shared session key to be established between the medium and a device authorized to access the content.

3. (previously presented) The medium of claim 1 is a digital versatile disc (DVD).

4. (previously presented) A device comprising:

an input/output apparatus to access a medium; and,

a processor communicatively coupled with the input/output apparatus, the processor being configured to

read a first media validation data from a writeable area of the medium,

set a first device validation data equal to the first media validation data,

read a second media validation data from a read only area of the medium,

set a second device validation data equal to the second media validation data,

compare the first device validation data and the second device validation data, and

deny authorization to access content stored on the medium if the first device validation data and the second device validation data are unequal.

5. (previously presented) The device of claim 4, wherein the processor is further configured to decrypt at least one of the first device validation data and the second device validation data and to deny authorization to access the content if a result of the decryption is unequal to a preselected value.

6. (previously presented) The device of claim 4, wherein the processor is further configured to:

establish a shared session key with the medium,

read a first media message authentication code from the medium,

set a first device message authentication code equal to the first media message authentication code,

calculate a second device message authentication code over the first media validation data using the shared session key,

compare the first device message authentication code and the second device message authentication code, and

deny authorization to access a content stored on the medium if the first device message authentication code and the second device message authentication code are unequal.

7. (original) The device of claim 4 is a digital versatile disc (DVD) player.

8. (previously presented) A data protection system, comprising:

a medium including (i) a writeable area that stores a first media validation data containing an encrypted preselected value and a content, (ii) a read only area of the medium that stores a second media validation data equal to the first media validation data.

a processor communicatively coupled with the medium, the processor being configured to read the first media validation data, set a first device validation data equal to the first media validation data, read the second media validation data, set a second device validation data equal to the second media validation data, compare the first device validation data and the second device validation data, and deny authorization to access the content if the first device validation data and the second device validation data are unequal.

9. (original) The data protection system of claim 8, further comprising:

a media circuit to calculate a media message authentication code over the second media validation data using a shared session key to be established when the processor attempts to access the content.

10. (previously presented) The data protection system of claim 8, wherein the processor is further configured to

establish a shared session key with the medium,

read a media message authentication code from the medium,

set a first device message authentication code equal to the media message authentication code,

calculate a second device message authentication code over the first device validation data using the shared session key,

compare the first and the second device message authentication codes and

deny authorization to access the content if the first and the second device message authentication codes are unequal.

11. (original) The data protection system of claim 8, wherein the reader is a digital versatile disc (DVD) player.

12. (previously presented) A method, comprising:

preselecting a value;

encrypting the preselected value;

setting a media validation data equal to the encrypted preselected value;

storing a first copy of the media validation data on a writeable area of a medium; and,

storing a second copy of the media validation data on a read only area of the medium to protect a content stored on the medium.

13. (previously presented) The method of claim 12, further comprising:

configuring a media processor to calculate a media message authentication code over the media validation data using a shared session key to be established when a media reader attempts to access the content.

14. (previously presented) The method of claim 12, further comprising:

configuring a media reader to read the media validation data from the writeable area of the medium;

setting a first device validation data equal to the media validation data read from the writeable area of the medium;

configuring the media reader to read the media validation data from the read only area of the medium;

setting a second device validation data equal to the media validation data read from the read only area of the medium;

configuring the media reader to compare the first device validation data and the second device validation data; and,

configuring the media reader to deny authorization to access the content if the first device validation data and the second device validation data are unequal.

15. (original) The method of claim 14, further comprising:

configuring the media reader to decrypt both the first device validation data and the second device validation data; and,

configuring the media reader to deny authorization to access the content if a result of the decryption is unequal to the preselected value.

16. (previously presented) The method of claim 12, wherein the medium is a digital versatile disc (DVD).

17. (currently amended) A tangible machine readable medium containing instructions which, when executed by an apparatus causes the apparatus to perform operations, comprising:

setting a validation data equal to an encrypted preselected value;

storing a first copy of the validation data on a writeable area of a medium; and,

storing a second copy of the validation data on a read only area of the medium.

18. (previously presented) The machine readable medium of claim 17, wherein the instructions, when executed, further cause the apparatus to perform operations comprising:

configuring a media processor to calculate a media message authentication code over the validation data using a shared session key to be established when a media reader attempts to access the content.

19. (original) The machine readable medium of claim 17 is a digital versatile disc (DVD).

20-22. (canceled)

23. (currently amended) A tangible machine readable medium, comprising:

a writeable area of the medium;

a read only area of the medium;

a content stored on the writeable area of the medium;~~,~~

a first media validation data containing an encrypted preselected value and being stored on the read only area; and

a second media validation data equal to the first media validation data and being stored on the writeable area.

24. (canceled)

25. (previously presented) The medium of claim 23, further comprising:

a circuit to calculate a media message authentication code over the first media validation data using a shared session key to be established between the medium and a device authorized to access the content.